

PATENT ABSTRACTS OF JAPAN

(11) Publication number : 11-205307
 (43) Date of publication of application : 30.07.1999

(51) Int.Cl. H04L 9/32
 G06F 13/00
 // G09C 1/00

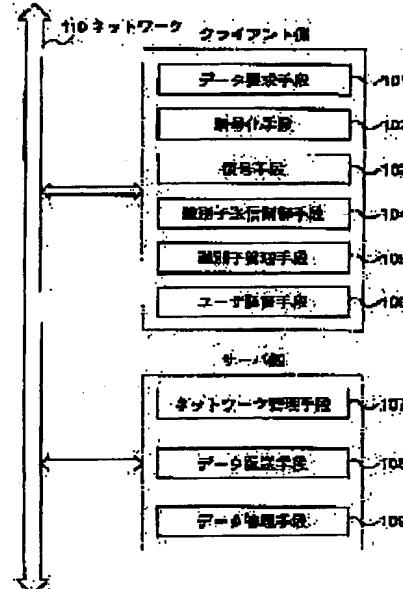
(21) Application number : 10-018281 (71) Applicant : CANON INC
 (22) Date of filing : 16.01.1998 (72) Inventor : TANAKA TETSUO

(54) INFORMATION PROCESSOR, NETWORK SYSTEM, RESOURCE IDENTIFIER CONVERSION METHOD AND STORAGE MEDIUM

(57) Abstract:

PROBLEM TO BE SOLVED: To save the procedure of ciphering and deciphering and to save the distribution procedure of a public key or a secret key by ciphering a resource identifier for specifying data on a network and deciphering it, based on a decipher key.

SOLUTION: An identifier management means 105 is operated so as to urge the input of a ciphered resource identifier (URL) and send the inputted and ciphered URL to a deciphering means 103. The deciphering means 103 deciphers the original URL from the ciphered URL and the decipher key, and if the deciphered URL is correct, delivers it to a client program. In the case the deciphering is not correctly performed or the deciphered URL is not correct, information for indicating incorrect user ID information is sent to the client program. Then, in the case the correct URL is delivered, protocol information, the host information of a server program and resource information on the server program, etc., are fetched so as to obtain a network resource, communication is performed with the server program and the network resource is obtained.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-205307

(43)公開日 平成11年(1999) 7月30日

(51) Int.Cl. [*]	識別記号	F I
H 04 L 9/32		H 04 L 9/00 6 7 3 Z
G 06 F 13/00	3 5 1	G 06 F 13/00 3 5 1 Z
// G 09 C 1/00	6 6 0	G 09 C 1/00 6 6 0 G

審査請求 未請求 請求項の数24 FD (全 16 頁)

(21)出願番号 特願平10-18281
 (22)出願日 平成10年(1998) 1月16日

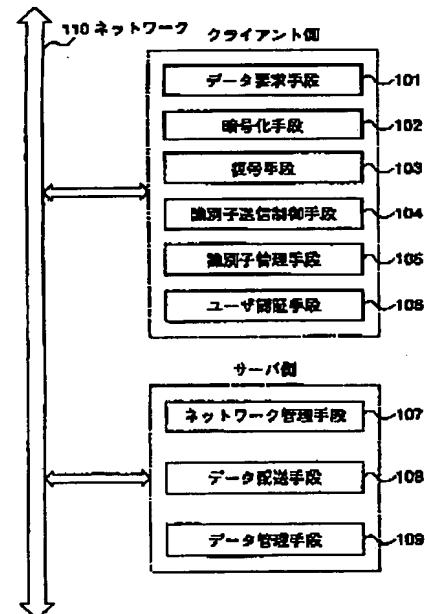
(71)出願人 000001007
 キヤノン株式会社
 東京都大田区下丸子3丁目30番2号
 (72)発明者 田中 哲郎
 東京都大田区下丸子3丁目30番2号 キヤ
 ノン株式会社内
 (74)代理人 弁理士 渡部 敏彦

(54)【発明の名称】 情報処理装置及びネットワークシステム並びにリソース識別子変換方法及び記憶媒体

(57)【要約】

【課題】 暗号鍵により暗号化されたリソース識別子を公開し、復号鍵及び元のリソース識別子をユーザ以外には非公開とすることにより、復号鍵により暗号化されたリソース識別子を復号できるユーザにのみアクセス可能にし、暗号化及び復号の手続きや認証のための公開鍵または秘密鍵を配布する手続きを節約すること等を可能とした情報処理装置及びネットワークシステム並びにリソース識別子変換方法及び記憶媒体を提供する。

【解決手段】 サーバにリソース識別子を用いデータ配送を要求するデータ要求手段101と、リソース識別子を暗号化する暗号化手段102と、リソース識別子を復号する復号手段103と、復号したリソース識別子が正しい時はサーバに送信し、正しくない時は送信しない識別子送信制御手段104と、入力されたリソース識別子を読み取り記憶する識別子管理手段105とを有する。



(2)

特開平11-205307

【特許請求の範囲】

【請求項 1】 ネットワークを介してサーバと通信可能な情報処理装置であって、

前記ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化手段と、暗号化したリソース識別子を復号鍵に基づき復号する復号手段とを有することを特徴とする情報処理装置。

【請求項 2】 前記サーバに対しリソース識別子を用いてデータ配達を要求するデータ要求手段と、前記復号したリソース識別子が正しい場合はリソース識別子を前記サーバに送信し、前記復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御手段とを有することを特徴とする請求項 1 記載の情報処理装置。

【請求項 3】 ユーザの認証を行うユーザ認証手段を有することを特徴とする請求項 1 又は 2 記載の情報処理装置。

【請求項 4】 前記ユーザ認証手段は、前記暗号化したリソース識別子が正しく復号された場合で且つ前記復号したリソース識別子から前記ネットワークを介してリソースを得られた場合はユーザを認証し、前記暗号化したリソース識別子が得られない場合又は前記暗号化したリソース識別子が正しく復号されない場合又は前記復号したリソース識別子から前記ネットワークを介してリソースを得られない場合はユーザを認証しないことを特徴とする請求項 3 記載の情報処理装置。

【請求項 5】 パスワードを復号鍵として記憶可能であることを特徴とする請求項 1 乃至 4 の何れかに記載の情報処理装置。

【請求項 6】 リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読み取り記憶する識別子管理手段を有し、前記リソース識別子は、World Wide Web サーバのアドレスを示す URL であることを特徴とする請求項 1 乃至 5 の何れかに記載の情報処理装置。

【請求項 7】 ネットワークを介してサーバ及びクライアント間で通信可能なネットワークシステムであって、前記クライアント側は、前記ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化手段と、暗号化したリソース識別子を復号鍵に基づき復号する復号手段とを有することを特徴とするネットワークシステム。

【請求項 8】 前記クライアント側は、前記サーバに対しリソース識別子を用いてデータ配達を要求するデータ要求手段と、前記復号したリソース識別子が正しい場合はリソース識別子を前記サーバに送信し、前記復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御手段とを有し、前記サーバ側は、前記ネットワークの上位装置名、アドレス、通信手段を管理するネットワーク管理手段と、該ネットワー-

ク管理手段による通信でデータを配達するデータ配達手段と、サーバ上のデータを管理するデータ管理手段とを有することを特徴とする請求項 7 記載のネットワークシステム。

【請求項 9】 前記クライアント側は、ユーザの認証を行うユーザ認証手段を有することを特徴とする請求項 7 又は 8 記載のネットワークシステム。

【請求項 10】 前記ユーザ認証手段は、前記暗号化したリソース識別子が正しく復号された場合で且つ前記復号したリソース識別子から前記ネットワークを介してリソースを得られた場合はユーザを認証し、前記暗号化したリソース識別子が得られない場合又は前記暗号化したリソース識別子が正しく復号されない場合又は前記復号したリソース識別子から前記ネットワークを介してリソースを得られない場合はユーザを認証しないことを特徴とする請求項 9 記載のネットワークシステム。

【請求項 11】 前記クライアント側は、パスワードを復号鍵として記憶可能であることを特徴とする請求項 7 乃至 10 の何れかに記載のネットワークシステム。

【請求項 12】 前記クライアント側は、リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読み取り記憶する識別子管理手段を有し、前記リソース識別子は、World Wide Web サーバのアドレスを示す URL であることを特徴とする請求項 7 乃至 11 の何れかに記載のネットワークシステム。

【請求項 13】 ネットワークを介してサーバと通信可能な情報処理装置におけるリソース識別子変換方法であって、

前記ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化ステップと、暗号化したリソース識別子を復号鍵に基づき復号する復号ステップとを有することを特徴とするリソース識別子変換方法。

【請求項 14】 前記サーバに対しリソース識別子を用いてデータ配達を要求するデータ読出ステップと、前記復号したリソース識別子が正しい場合はリソース識別子を前記サーバに送信し、前記復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御ステップとを有することを特徴とする請求項 13 記載のリソース識別子変換方法。

【請求項 15】 ユーザの認証を行うユーザ認証ステップを有することを特徴とする請求項 13 又は 14 記載のリソース識別子変換方法。

【請求項 16】 前記ユーザ認証ステップでは、前記暗号化したリソース識別子が正しく復号された場合で且つ前記復号したリソース識別子から前記ネットワークを介してリソースを得られた場合はユーザを認証し、前記暗号化したリソース識別子が得られない場合又は前記暗号化したリソース識別子が正しく復号されない場合又は前記復号したリソース識別子から前記ネットワークを介し

(3)

特開平 11-205307

でリソースを得られない場合はユーザを認証しないことを特徴とする請求項 15 記載のリソース識別子変換方法。

【請求項 17】 パスワードを復号鍵として記憶可能であることを特徴とする請求項 13 乃至 16 の何れかに記載のリソース識別子変換方法。

【請求項 18】 リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読み取り記憶する識別子管理ステップを有し、前記リソース識別子は、World Wide Web サーバのアドレスを示す URL であることを特徴とする請求項 13 乃至 17 の何れかに記載のリソース識別子変換方法。

【請求項 19】 ネットワークを介してサーバと通信可能な情報処理装置に供給可能な記憶媒体であつて、前記ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化ステップと、暗号化したリソース識別子を復号鍵に基づき復号する復号ステップとを有するプログラムを記憶したことを特徴とする記憶媒体。

【請求項 20】 前記プログラムは、前記サーバに対しリソース識別子を用いてデータ配達を要求するデータ読み出ステップと、前記復号したリソース識別子が正しい場合はリソース識別子を前記サーバに送信し、前記復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御ステップとを有することを特徴とする請求項 19 記載の記憶媒体。

【請求項 21】 前記プログラムは、ユーザの認証を行うユーザ認証ステップを有することを特徴とする請求項 19 又は 20 記載の記憶媒体。

【請求項 22】 前記ユーザ認証ステップでは、前記暗号化したリソース識別子が正しく復号された場合で且つ前記復号したリソース識別子から前記ネットワークを介してリソースを得られた場合はユーザを認証し、前記暗号化したリソース識別子が得られない場合又は前記暗号化したリソース識別子が正しく復号されない場合又は前記復号したリソース識別子から前記ネットワークを介してリソースを得られない場合はユーザを認証しないことを特徴とする請求項 21 記載の記憶媒体。

【請求項 23】 パスワードを復号鍵として記憶可能であることを特徴とする請求項 19 乃至 22 の何れかに記載の記憶媒体。

【請求項 24】 前記プログラムは、リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読み取り記憶する識別子管理ステップを有し、前記リソース識別子は、World Wide Web サーバのアドレスを示す URL であることを特徴とする請求項 19 乃至 23 の何れかに記載の記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、情報処理装置及び

ネットワークシステム並びにリソース識別子変換方法及び記憶媒体に係り、更に詳しく述べては、クライアント・サーバ方式によりネットワークを介してデータを送受信する場合に用いて好適な情報処理装置及びネットワークシステム並びにリソース識別子変換方法及び記憶媒体に関するもの。

【0002】

【従来の技術】 従来、インターネットを介したデータ送受信方法は、TCP (Transmission Control Protocol : ネットワークのトランスポート層の通信プロトコル) / UDP (User Datagram Protocol : 信頼性を保証しないトランスポート層の通信プロトコル) / IP (Internet Protocol : インターネット層の通信プロトコル) 上のプロトコルを利用したプログラムを使用して行われてきた。その際、ネットワーク上のリソースは、<プロトコルの種類、リソースを提供するサーバを指定する識別子、サーバ上のリソースを指定する識別子>からなる組により決定されている。

【0003】 また、サーバのポート番号やサーバ上のユーザ名及び暗号化されたパスワード等の情報も付加的に指定することができる。特に、リソース識別子として URL (Uniform Resource Locator : World Wide Web サーバのアドレス) を利用した場合には、
scheme://user:password@host:port/url-path
のように、スキーム (scheme) と呼ぶプロトコルの種類を指定する部分と、ユーザ名を指定するユーザ (user) 部、パスワードを指定するパスワード (password) 部、ホスト名を指定するホスト (host) 部、ポート番号を指定するポート (port) 部、サーバ上のリソースを指定する URL パス (url-path) 部、により構成されている。但し、ユーザ部、パスワード部、ポート部、URL パス部は、デフォルトとして預め指定されているものを使用する場合はそれぞれ省略可能である。

【0004】 また、インターネットを介したデータ送受信において情報のセキュリティを高めるためには、プロトコル自身に暗号化及び認証機能を付加したり、データそのものを暗号化したりするよう構成されている。また、通常のプロトコルを使用してデータそのものを暗号化しない方法として、パスワードを利用した認証機能がある。これは、リソース識別子を指定してリソースを得る際に、ユーザを確認する文字列の入力を促し、正しい文字列が入力された場合にリソースを送信するものである。

【0005】

【発明が解決しようとする課題】 しかしながら、上述した従来技術では、パスワードを付けたリソース識別子 (URL) にアクセスする場合、クライアントからサーバにリソース識別子 (URL) が送信されると、サーバ

(4)

特開平11-205307

からクライアントにユーザ確認の応答が返され、次に、クライアントはユーザに対して、ユーザ名やパスワード等を入力するためのパネル等を表示してユーザ名やパスワード等を得ていた。正しくユーザ名やパスワード等を得られた場合は、クライアントはサーバにユーザ名やパスワード等を送信し、サーバは送信されたユーザ名やパスワード等を確認し、認証された場合に、認証情報と所望のリソースを送信していた。

【0006】また、従来技術では、パスワードを付けたリソース識別子（URL）にアクセスする場合、暗号化機能を付加したプロトコルを利用するか、またはデータを暗号化する方法を除いて、パスワードそのものが暗号化されずにネットワークを流れるという欠点があった。そのため、ネットワークを流れるパケットを盗聴することにより悪意のあるユーザによりパスワードが盗まれる恐れがあった。更に、従来技術では、パスワードを付けたリソース識別子（URL）にアクセスする場合、アクセス毎またはセッション毎にパスワードを入力する必要があった。

【0007】即ち、上述した如く従来技術においては、リソース識別子が暗号化されていないため、認証を行うためには、サーバ側のパスワード機構やクライアント側のサイトのアドレス等を検査して認証を行う必要があった。また、リソース識別子とユーザのデジタル署名機構が独立であったため、ユーザの認証を行うためには、プロトコル自体に暗号化及び認証機能を付加した技術が必要であった。また、データを暗号化して送受信する場合には、復号鍵の配達やデータの復号を行う必要があった。

【0008】本発明は、上述した点に鑑みなされたものであり、暗号鍵により暗号化されたリソース識別子（URL）を公開し、復号鍵及び元のリソース識別子（URL）をユーザ以外には非公開することにより、復号鍵により暗号化されたリソース識別子（URL）を復号できるユーザにのみアクセス可能にし、暗号化及び復号の手続きや認証のための公開鍵または秘密鍵を配布する手続きを簡約すること等を可能とした情報処理装置及びネットワークシステム並びにリソース識別子変換方法及び記憶媒体を提供することを第1の目的とする。

【0009】また、本発明は、上述した点に鑑みなされたものであり、暗号化されたリソース識別子（URL）を使用する際に、特定のソフトウェアを使用するように強制することにより、ソフトウェアが暗号化鍵及び復号鍵を管理し、ネットワーク上のリソースを送受信すると共に、ユーザのライセンス処理をも同時に行うことを可能とした情報処理装置及びネットワークシステム並びにリソース識別子変換方法及び記憶媒体を提供することを第2の目的とする。

【0010】

【課題を解決するための手段】上記目的を達成するた

め、請求項1の発明は、ネットワークを介してサーバと通信可能な情報処理装置であって、前記ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化手段と、暗号化したリソース識別子を復号鍵に基づき復号する復号手段とを有することを特徴とする。

【0011】上記目的を達成するため、請求項2の発明は、前記サーバに対しリソース識別子を用いてデータ配送を要求するデータ要求手段と、前記復号したリソース識別子が正しい場合はリソース識別子を前記サーバに送信し、前記復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御手段とを有することを特徴とする。

【0012】上記目的を達成するため、請求項3の発明は、ユーザの認証を行うユーザ認証手段を有することを特徴とする。

【0013】上記目的を達成するため、請求項4の発明は、前記ユーザ認証手段は、前記暗号化したリソース識別子が正しく復号された場合で且つ前記復号したリソース識別子から前記ネットワークを介してリソースを得られた場合はユーザを認証し、前記暗号化したリソース識別子が得られない場合又は前記暗号化したリソース識別子が正しく復号されない場合又は前記復号したリソース識別子から前記ネットワークを介してリソースを得られない場合はユーザを認証しないことを特徴とする。

【0014】上記目的を達成するため、請求項5の発明は、パスワードを復号鍵として記憶可能であることを特徴とする。

【0015】上記目的を達成するため、請求項6の発明は、リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読み取り記憶する識別子管理手段を有し、前記リソース識別子は、World Wide Webサーバのアドレスを示すURLであることを見出する。

【0016】上記目的を達成するため、請求項7の発明は、ネットワークを介してサーバ及びクライアント間で通信可能なネットワークシステムであって、前記クライアント側は、前記ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化手段と、暗号化したリソース識別子を復号鍵に基づき復号する復号手段とを有することを特徴とする。

【0017】上記目的を達成するため、請求項8の発明は、前記クライアント側は、前記サーバに対しリソース識別子を用いてデータ配送を要求するデータ要求手段と、前記復号したリソース識別子が正しい場合はリソース識別子を前記サーバに送信し、前記復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御手段とを有し、前記サーバ側は、前記ネットワークの上位装置名、アドレス、通信手段を管理するネットワーク管理手段と、該ネットワーク管理手

(5)

特開平11-205307

段による通信でデータを配達するデータ配達手段と、サーバ上のデータを管理するデータ管理手段とを有することを特徴とする。

【0018】上記目的を達成するため、請求項9の発明は、前記クライアント側は、ユーザの認証を行うユーザ認証手段を有することを特徴とする。

【0019】上記目的を達成するため、請求項10の発明は、前記ユーザ認証手段は、前記暗号化したリソース識別子が正しく復号された場合で且つ前記復号したリソース識別子から前記ネットワークを介してリソースを得られた場合はユーザを認証し、前記暗号化したリソース識別子が得られない場合又は前記暗号化したリソース識別子が正しく復号されない場合又は前記復号したリソース識別子から前記ネットワークを介してリソースを得られない場合はユーザを認証しないことを特徴とする。

【0020】上記目的を達成するため、請求項11の発明は、前記クライアント側は、パスワードを復号盤として記憶可能であることを特徴とする。

【0021】上記目的を達成するため、請求項12の発明は、前記クライアント側は、リソース識別子の入力を促す旨を表示すると共に入力されたりソース識別子を読み取り記憶する識別子管理手段を有し、前記リソース識別子は、World Wide Webサーバのアドレスを示すURLであることを特徴とする。

【0022】上記目的を達成するため、請求項13の発明は、ネットワークを介してサーバと通信可能な情報処理装置におけるリソース識別子変換方法であって、前記ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化ステップと、暗号化したリソース識別子を復号鍵に基づき復号する復号ステップとを有することを特徴とする。

【0023】上記目的を達成するため、請求項14の発明は、前記サーバに対しリソース識別子を用いてデータ配達を要求するデータ読出ステップと、前記復号したりソース識別子が正しい場合はリソース識別子を前記サーバに送信し、前記復号したりソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御ステップとを有することを特徴とする。

【0024】上記目的を達成するため、請求項15の発明は、ユーザの認証を行うユーザ認証ステップを有することを特徴とする。

【0025】上記目的を達成するため、請求項16の発明は、前記ユーザ認証ステップでは、前記暗号化したリソース識別子が正しく復号された場合で且つ前記復号したりソース識別子から前記ネットワークを介してリソースを得られた場合はユーザを認証し、前記暗号化したリソース識別子が得られない場合又は前記暗号化したリソース識別子が正しく復号されない場合又は前記復号したりソース識別子から前記ネットワークを介してリソースを得られない場合はユーザを認証しないことを特徴とする。

る。

【0026】上記目的を達成するため、請求項17の発明は、パスワードを復号鍵として記憶可能であることを特徴とする。

【0027】上記目的を達成するため、請求項18の発明は、リソース識別子の入力を促す旨を表示すると共に入力されたりソース識別子を読み取り記憶する識別子管理ステップを有し、前記リソース識別子は、World Wide Webサーバのアドレスを示すURLであることを特徴とする。

【0028】上記目的を達成するため、請求項19の発明は、ネットワークを介してサーバと通信可能な情報処理装置に供給可能な記憶媒体であって、前記ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化ステップと、暗号化したリソース識別子を復号鍵に基づき復号する復号ステップとを有するプログラムを記憶したことを特徴とする。

【0029】上記目的を達成するため、請求項20の発明は、前記プログラムは、前記サーバに対しリソース識別子を用いてデータ配達を要求するデータ読出ステップと、前記復号したりソース識別子が正しい場合はリソース識別子を前記サーバに送信し、前記復号したりソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御ステップとを有することを特徴とする。

【0030】上記目的を達成するため、請求項21の発明は、前記プログラムは、ユーザの認証を行うユーザ認証ステップを有することを特徴とする。

【0031】上記目的を達成するため、請求項22の発明は、前記ユーザ認証ステップでは、前記暗号化したリソース識別子が正しく復号された場合で且つ前記復号したりソース識別子から前記ネットワークを介してリソースを得られた場合はユーザを認証し、前記暗号化したリソース識別子が得られない場合又は前記暗号化したリソース識別子が正しく復号されない場合又は前記復号したりソース識別子から前記ネットワークを介してリソースを得られない場合はユーザを認証しないことを特徴とする。

【0032】上記目的を達成するため、請求項23の発明は、パスワードを復号鍵として記憶可能であることを特徴とする。

【0033】上記目的を達成するため、請求項24の発明は、前記プログラムは、リソース識別子の入力を促す旨を表示すると共に入力されたりソース識別子を読み取り記憶する識別子管理ステップを有し、前記リソース識別子は、World Wide Webサーバのアドレスを示すURLであることを特徴とする。

【0034】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。

【0035】 [1] 第1の実施の形態

図2は本発明の第1の実施の形態及び後述する第2の実施の形態に係る情報処理装置(クライアント)の構成を示すブロック図である。本発明の第1の実施の形態に係る情報処理装置は、入力部201と、中央演算処理部202と、主記憶部203と、読み出し専用メモリ204と、二次記憶部205と、出力部206と、ネットワークインターフェース207とを備える構成となっている。

【0036】 上記各部の構成を詳述すると、入力部201は、キーボードやマウス等から構成されており、各種データの入力や指示を行う際に使用される。中央演算処理部202は、入力部201、主記憶部203、読み出し専用メモリ204、二次記憶部205、出力部206、ネットワークインターフェース207を統括的に制御するものであり、後述する図3のクライアントプログラム301、暗号化プログラム302、復号プログラム304の実行等を制御することにより、後述する図4及び図5のフローチャートに示す処理を実行する。

【0037】 主記憶部203は、中央演算処理部202による命令実行やデータ操作等を行う際に使用される記憶部である。読み出し専用メモリ204は、システムプログラム等を記憶する読み出し専用の記憶部である。二次記憶部205は、例えばハードディスク或いはフロッピディスク等から構成されており、主記憶部203の容量不足を補う辅助記憶部である。出力部206は、端末やプリンタ等から構成されており、データの表示や印刷等の出力を実行する。ネットワークインターフェース207は、ネットワーク上に接続された外部装置との間におけるデータの送受信を行う。

【0038】 図3は本発明の第1の実施の形態及び後述する第2の実施の形態に係る情報処理装置(クライアント)及び外部装置(サーバ)からなるネットワークシステムの構成を示すブロック図である。本発明の第1の実施の形態に係るネットワークシステムは、クライアントプログラム301、暗号化プログラム302、暗号化鍵E・303、復号プログラム304、復号鍵D・305、ネットワークインターフェース306、ネットワーク307、ネットワークインターフェース308、サーバプログラム309、送信データ310から構成されている。クライアント側は、クライアントプログラム301～ネットワークインターフェース306を備えており、サーバ側は、ネットワークインターフェース308、サーバプログラム309を備えている。

【0039】 上記各部の構成を詳述すると、クライアントプログラム301は、ネットワーク307を介してサーバ側から送信されてくるデータを受信する機能を有するプログラムである。暗号化プログラム302は、リソース識別子(URL)を暗号化するプログラムである。暗号化鍵E・303は、リソース識別子(URL)の暗号化に使用する。復号プログラム304は、暗号化され

たリソース識別子(URL)を復号する復号プログラムである。復号鍵D・305は、リソース識別子(URL)の復号に使用する。ネットワークインターフェース306は、クライアント側のネットワークインターフェースであり、ネットワーク307を介してサーバ側とデータの送受信を行う。

【0040】 ネットワーク307は、クライアント及びサーバ間におけるデータの通信経路である。ネットワークインターフェース308は、サーバ側のネットワークインターフェースであり、ネットワーク307を介してクライアント側とデータの送受信を行う。サーバプログラム309は、ネットワーク307を介してサーバ側からクライアント側へデータを送信する機能を有するプログラムである。送信データ310は、サーバ側からクライアント側へ送信されるデータである。

【0041】 図1は本発明の第1の実施の形態及び後述する第2の実施の形態に係る情報処理装置(クライアント)及び外部装置(サーバ)からなるネットワークシステムの要部の構成を示すと共に特許請求の範囲に対応させた機能ブロック図である。情報処理装置(クライアント)は、データ要求手段101、暗号化手段102、復号手段103、識別子送信制御手段104、識別子管理手段105、ユーザ認証手段106を備え、外部装置(サーバ)は、ネットワーク管理手段107、データ配信手段108、データ管理手段109を備えている。この場合、ユーザ認証手段106以外の各手段は第1及び第2の実施の形態に共通の構成要件であり、ユーザ認証手段106は第2の実施の形態に係る構成要件である。尚、図1の構成は一例であり図示の構成に限定されるものではない。

【0042】 上記各部の機能を詳述すると、クライアント側のデータ要求手段101は、サーバに対してURL等のネットワーク110上のデータを指定するリソース識別子を用いてデータ配信を要求する。暗号化手段102は、ネットワーク110上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する。復号手段103は、暗号化したデータまたはデータを指定するリソース識別子を復号鍵に基づき復号する。識別子送信制御手段104は、復号したリソース識別子が正しい場合はリソース識別子をサーバに送信し、復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない。識別子管理手段105は、リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読み取り記憶する。

【0043】 また、サーバ側のネットワーク管理手段107は、ネットワーク110のホスト名、アドレス、通信手段の管理を行う。データ配信手段108は、ネットワーク管理手段107を用いて通信することによりデータの配信を行う。データ管理手段109は、サーバ上のデータの管理を行う。

(7)

特開平11-205307

【0044】尚、データ要求手段101、識別子送信制御手段104、識別子管理手段105、ユーザ認証手段106は、上記図3のクライアントプログラム301に対応し、暗号化手段102は、上記図3の暗号化プログラム302に対応し、復号手段103は、上記図3の復号プログラム304に対応する。また、ネットワーク管理手段107、データ配送手段108、データ管理手段109は、上記図3のサーバプログラム309に対応する。

【0045】図7は本発明の第1の実施の形態及び後述する第2の実施の形態に係るプログラム及び関連データが記憶媒体から情報処理装置へ供給される概念例を示す説明図である。本発明のプログラム及び関連データは、記憶媒体701（例えばフロッピディスク或いはCD-ROM等）を情報処理装置702に装備された記憶媒体ドライブの挿入口703に挿入することで供給される。

【0046】本発明のプログラム及び関連データを記憶媒体701から一旦、二次記憶部205（例えばハードディスク）へインストールすることにより、二次記憶部205から主記憶部203（例えばRAM）にロードし、本発明のプログラムを実行することが可能となる。但し、二次記憶部205へインストールせずに直接、記憶媒体701から主記憶部203にロードし、本発明のプログラムを実行することも可能である。

【0047】図6は本発明の第1の実施の形態及び後述する第2の実施の形態に係るプログラム及び関連データを記憶した記憶媒体の記憶内容の構成例を示す説明図である。記憶媒体（フロッピディスク或いはCD-ROM等）は、例えばボリューム情報601、ディレクトリ情報602、プログラム実行ファイル603、プログラム関連データファイル604等の記憶内容で構成される。本発明のプログラムは、後述する図4及び図5のフローチャートに基づきプログラムコード化されたものである。

【0048】次に、上記の如く構成してなる本発明の第1の実施の形態に係る情報処理装置（クライアント）及び外部装置（サーバ）からなるネットワークシステムにおける情報処理装置（クライアント）の中央演算処理部202により制御されるクライアント側の処理の流れについて、図4のフローチャートを参照しながら説明する。

【0049】情報処理装置（クライアント）側のクライアントプログラム301は、本処理が開始すると開始したユーザに対して、暗号化プログラム302により暗号化鍵303を用いて暗号化されたリソース識別子（URL）を入力するウインドウを表示する（ステップS401）。次に、暗号化されたリソース識別子（URL）が得られたか否かを判断する（ステップS402）。暗号化されたリソース識別子（URL）が得られない場合は、本処理を終了する。他方、暗号化されたリソース識

別子（URL）が得られた場合は、復号鍵305を得る（ステップS403）。

【0050】復号プログラム304は、暗号化されたリソース識別子（URL）を復号鍵305を使用して復号する（ステップS404）。次に、復号したリソース識別子（URL）からプロトコル情報やサーバ情報やサーバのリソース情報を得て、サーバプログラム309とネットワーク307を介してサーバ側と通信を行う（ステップS405）。次に、サーバプログラム309との通信により、上記復号したリソース識別子（URL）で指定したデータをサーバ側から得られたか否かを判断する（ステップS406）。

【0051】上記復号したリソース識別子（URL）で指定したデータをサーバ側から得られなかった場合は、本処理を終了する。他方、上記復号したリソース識別子（URL）で指定したデータをサーバ側から得られた場合は、リソース識別子（URL）から得られたデータをネットワークのリソースとして表示し（ステップS407）、本処理を終了する。

【0052】以上説明したように、本発明の第1の実施の形態によれば、ネットワークシステムの情報処理装置は、サーバに対しリソース識別子を用いてデータ配達を要求するデータ要求手段101と、ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化手段102と、暗号化したリソース識別子を復号鍵に基づき復号する復号手段103と、復号したリソース識別子が正しい場合はリソース識別子をサーバに送信し、復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御手段104と、リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読み取り記憶する識別子管理手段105とを有するため、下記のような効果を奏する。

【0053】上記の構成により、本発明の第1の実施の形態では、識別子管理手段105は、クライアントプログラムを使用するユーザに対して、暗号化されたリソース識別子（URL）の入力を促し、入力され暗号化されたリソース識別子（URL）を復号手段103に送るよう動作する。復号手段103は、暗号化されたリソース識別子（URL）と復号鍵から元のリソース識別子（URL）を復号し、復号されたリソース識別子（URL）が正しいものである場合には、クライアントプログラムに正しいリソース識別子（URL）を渡すように動作する。

【0054】上記暗号化されたリソース識別子（URL）から正しく復号されない場合、または復号されたリソース識別子（URL）情報が正しいものでない場合には、不正なユーザID情報を示す情報をクライアントプログラムに送るように動作する。クライアントプログラムは、正しいリソース識別子（URL）情報を渡された

(8)

特開平11-205307

場合には、リソース識別子（URL）情報から、ネットワークリソースを得るためにプロトコル情報やサーバプログラムのホスト情報、サーバプログラム上のリソース情報等を取り出し、サーバプログラムと通信し、ネットワークリソースを得るように動作する。

【0055】従って、本発明の第1の実施の形態の効果を箇条書きにすると下記のようになる。

【0056】(1) データそのものを暗号化したり復号したりする必要がないため、暗号化及び復号の手続きを節約できるという効果がある。また、認証のための公開鍵または秘密鍵を配布する手続きを節約できるという効果がある。

【0057】(2) パスワードを用いた認証機構に対して、ネットワークの通信回数を減らすことにより、ネットワークのトラフィック（通信量）及び通信時間を軽減できるという効果がある。即ち、上述した従来技術と比較すると、本発明では、暗号化されたリソース識別子（URL）を使用する場合は、クライアントがリソース識別子（URL）を復号し、正しければ復号したリソース識別子（URL）をサーバに送信し、正しくなければリソース識別子（URL）を送信しないため、通信回数が軽減されるという効果がある。

【0058】(3) パスワードを用いた認証機構に対して、パスワードをネットワークに流すことがなくなるという効果がある。即ち、上述した従来技術と比較すると、本発明では、パスワードや暗号の暗号化鍵、復号鍵そのものはネットワークに流れないので、従来技術のようなパスワードの盗難といった危険を回避することが可能になるという効果がある。

【0059】(4) パスワードを用いた認証機構に対して、パスワードをアクセス毎に入力する手間が軽減されるという効果がある。即ち、上述した従来技術と比較すると、本発明では、クライアントがパスワードを復号鍵として記憶するので、一回だけクライアントにリソース識別子（URL）と復号鍵を登録すると、次回からはユーザがパスワードを入力する必要がなくなるという効果がある。

【0060】(5) パスワードを用いた認証機構に対して、ユーザがパスワードを記憶する必要がなくなるという効果がある。

【0061】(6) パスワードを用いた認証機構に対して、ユーザがパスワードを誤入力する恐れがなくなるという効果がある。

【0062】[2] 第2の実施の形態

本発明の第2の実施の形態に係る情報処理装置（クライアント）は、上記第1の実施の形態と同様に、入力部201と、中央演算処理部202と、主記憶部203と、読み出し専用メモリ204と、二次記憶部205と、出力部206と、ネットワークインタフェース207とを備える構成となっている（上記図2参照）。

【0063】また、本発明の第2の実施の形態に係る情報処理装置（クライアント）及び外部装置（サーバ）からなるネットワークシステムは、上記第1の実施の形態と同様に、クライアントプログラム301、暗号化プログラム302、暗号化鍵E・303、復号プログラム304、復号鍵D・305、ネットワークインタフェース306、ネットワーク307、ネットワークインタフェース308、サーバプログラム309、送信データ310から構成されている（上記図3参照）。

【0064】また、本発明の第2の実施の形態に係る情報処理装置（クライアント）及び外部装置（サーバ）から構成されると共に特許請求の範囲に対応させたネットワークシステムの情報処理装置（クライアント）は、データ要求手段101、暗号化手段102、復号手段103、識別子送信制御手段104、識別子管理手段105、ユーザ認証手段106を備え、外部装置（サーバ）は、ネットワーク管理手段107、データ配達手段108、データ管理手段109を備えている（上記図1参照）。即ち、第2の実施の形態の情報処理装置（クライアント）は、上記第1の実施の形態の各手段101～105にユーザ認証手段106を追加した構成となっている。

【0065】ユーザ認証手段106は、暗号化されたりソース識別子が正しく復号された場合で且つ復号されたリソース識別子からネットワーク110を介してリソースを得られた場合はユーザを認証し、暗号化されたリソース識別子が得られない場合、または暗号化されたリソース識別子が正しく復号されない場合、または復号されたりソース識別子からネットワーク110を介してリソースを得られない場合はユーザを認証しない。

【0066】また、本発明の第2の実施の形態に係る処理プログラム及び関連データは、上記第1の実施の形態と同様に、記憶媒体701（例えばフロッピディスク或いはCD-ROM等）を情報処理装置702に装備された記憶媒体ドライブ703に挿入することで供給される（上記図4参照）。

【0067】また、本発明の第2の実施の形態に係る処理プログラム及び関連データを記憶した記憶媒体（フロッピディスク或いはCD-ROM等）は、上記第1の実施の形態と同様に、例えばボリューム情報601、ディレクトリ情報602、プログラム実行ファイル603、プログラム関連データファイル604等の記憶内容で構成される（上記図6参照）。上記の図1～図3、図6～図7の各部の構成は上記第1の実施の形態で詳述したので説明を省略する。

【0068】次に、上記の如く構成してなる本発明の第2の実施の形態に係る情報処理装置（クライアント）及び外部装置（サーバ）からなるネットワークシステムにおける情報処理装置（クライアント）の中央演算処理部202により制御されるクライアント側の処理の流れに

(9)

特開平11-205307

ついて、図5のフローチャートを参照しながら説明する。

【0069】情報処理装置（クライアント）側のクライアントプログラム301は、本処理が開始すると開始したユーザに対して、暗号化プログラム302により暗号化鍵303を用いて暗号化されたリソース識別子（URL）を入力するウインドウを表示する（ステップS501）。次に、暗号化されたリソース識別子（URL）が得られたか否かを判断する（ステップS502）。暗号化されたリソース識別子（URL）が得られない場合は、ステップS508へ移行する。他方、暗号化されたリソース識別子（URL）が得られた場合は、復号鍵305を得る（ステップS503）。

【0070】復号プログラム304は、暗号化されたリソース識別子（URL）を復号鍵305を使用して復号する（ステップS504）。次に、復号したリソース識別子（URL）からプロトコル情報やサーバ情報やサーバのリソース情報を得て、サーバプログラム309とネットワーク307を介してサーバ側と通信を行う（ステップS506）。次に、サーバプログラム309との通信により、上記復号したリソース識別子（URL）で指定したデータをサーバ側から得られたか否かを判断する（ステップS506）。

【0071】上記復号したリソース識別子（URL）で指定したデータをサーバ側から得られた場合は、ユーザの認証を行う（ステップS507）。更に、リソース識別子（URL）から得られたデータをネットワークのリソースとして表示し（ステップS509）、本処理を終了する。他方、上記復号したリソース識別子（URL）で指定したデータをサーバ側から得られなかった場合は、ユーザの認証を行わず（ステップS508）、本処理を終了する。

【0072】以上説明したように、本発明の第2の実施の形態によれば、ネットワークシステムの情報処理装置は、サーバに対しリソース識別子を用いてデータ配送を要求するデータ要求手段101と、ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化手段102と、暗号化したリソース識別子を復号鍵に基づき復号する復号手段103と、復号したリソース識別子が正しい場合はリソース識別子をサーバに送信し、復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御手段104と、リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読み取り記憶する識別子管理手段105と、暗号化したリソース識別子が正しく復号された場合で且つ復号したリソース識別子からネットワークを介してリソースを得られた場合はユーザを認証し、暗号化したリソース識別子が得られない場合、または暗号化したリソース識別子が正しく復号されない場合、または復号したリソース識別子からネットワークを

介してリソースを得られない場合はユーザを認証しないユーザ認証手段106とを有するため、下記のような効果を奏する。

【0073】上記の構成により、本発明の第2の実施の形態では、上記第1の実施の形態と同様の動作を行うと共に、更に、上記のユーザ認証手段106は、上記の如く、暗号化されたリソース識別子（URL）が正しく復号された場合、且つ復号されたリソース識別子（URL）からネットワークを介してリソースを得られた場合にユーザを認証し、暗号化されたリソース識別子（URL）が得られない場合、または暗号化されたリソース識別子（URL）が正しく復号されない場合、または復号されたリソース識別子（URL）からネットワークを介してリソースを得られない場合にユーザを認証しないよう動作する。

【0074】従って、本発明の第2の実施の形態の効果を箇条書きにすると上記第1の実施の形態と同様に下記のようになる。

【0075】（1）データそのものを暗号化したり復号したりする必要がないため、暗号化及び復号の手続きを節約できるという効果がある。また、認証のための公開鍵または秘密鍵を配布する手続きを節約できるという効果がある。

【0076】（2）パスワードを用いた認証機構に対して、ネットワークの通信回数を減らすことにより、ネットワークのトラフィック（通信量）及び通信時間を軽減できるという効果がある。即ち、上述した従来技術と比較すると、本発明では、暗号化されたリソース識別子（URL）を使用する場合は、クライアントがリソース識別子（URL）を復号し、正しければ復号したリソース識別子（URL）をサーバに送信し、正しくなければリソース識別子（URL）を送信しないため、通信回数が軽減されるという効果がある。

【0077】（3）パスワードを用いた認証機構に対して、パスワードをネットワークに流すことがなくなるという効果がある。即ち、上述した従来技術と比較すると、本発明では、パスワードや暗号の暗号化鍵、復号鍵そのものはネットワークに流れないため、従来技術のようなパスワードの盗難といった危険を回避することが可能になるという効果がある。

【0078】（4）パスワードを用いた認証機構に対して、パスワードをアクセス毎に入力する手間が軽減されるという効果がある。即ち、上述した従来技術と比較すると、本発明では、クライアントがパスワードを復号鍵として記憶するので、一回だけクライアントにリソース識別子（URL）と復号鍵を登録すると、次回からはユーザがパスワードを入力する必要がなくなるという効果がある。

【0079】（5）パスワードを用いた認証機構に対して、ユーザがパスワードを記憶する必要がなくなるとい

(10)

特開平11-205307

う効果がある。

【0080】(6) パスワードを用いた認証機構に対して、ユーザがパスワードを誤入力する恐れがなくなるという効果がある。

【0081】尚、本発明は、複数の機器から構成されるシステムに適用しても、1つの機器からなる装置に適用してもよい。前述した実施形態の機能を実現するソフトウェアのプログラムコードを記憶した記憶媒体を、システム或いは装置に供給し、そのシステム或いは装置のコンピュータ（またはCPUやMPU）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。

【0082】この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【0083】プログラムコードを供給するための記憶媒体としては、例えば、フロッピディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、CD-R、磁気テープ、不揮発性のメモリカード、ROMなどを用いることができる。

【0084】また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているOSなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【0085】更に、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるCPUなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【0086】

【発明の効果】以上説明したように、請求項1の発明によれば、ネットワークを介してサーバと通信可能な情報処理装置であって、前記ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化手段と、暗号化したリソース識別子を復号鍵に基づき復号する復号手段とを有するため、下記のような効果を奏する。

【0087】データそのものを暗号化したり復号したりする必要がないため、暗号化及び復号の手続きを節約できると共に、認証のための公開鍵または秘密鍵を配布する手続きを節約できるという効果がある。

【0088】また、パスワードを用いた認証機構に対して、パスワードをネットワークに流すことがなくなると

いう効果がある。即ち、上述した従来技術と比較すると、本発明では、パスワードや暗号の暗号化鍵、復号鍵そのものはネットワークに流れないので、従来技術のようなパスワードの盗難といった危険を回避することが可能になるという効果がある。

【0089】請求項2の発明によれば、情報処理装置は、前記サーバに対しリソース識別子を用いてデータ配送を要求するデータ要求手段と、前記復号したリソース識別子が正しい場合はリソース識別子を前記サーバに送信し、前記復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御手段とを有するため、下記のような効果を奏する。

【0090】上記請求項1の発明と同様の効果があるばかりでなく、パスワードを用いた認証機構に対して、ネットワークの通信回数を減らすことにより、ネットワークのトラフィック（通信量）及び通信時間を軽減できるという効果がある。即ち、上述した従来技術と比較すると、本発明では、暗号化されたリソース識別子を使用する場合は、クライアントがリソース識別子を復号し、正しければ復号したリソース識別子をサーバに送信し、正しくなければリソース識別子を送信しないため、通信回数が軽減されるという効果がある。

【0091】請求項3の発明によれば、情報処理装置は、ユーザの認証を行うユーザ認証手段を有するため、下記のような効果を奏する。

【0092】上記請求項1及び請求項2の発明と同様に、暗号化及び復号の手続きを節約できる、認証のための公開鍵または秘密鍵を配布する手続きを節約できる、パスワードの盗難といった危険を回避することが可能になる、通信回数が軽減される等の効果がある。

【0093】請求項4の発明によれば、情報処理装置の前記ユーザ認証手段は、前記暗号化したリソース識別子が正しく復号された場合で且つ前記復号したリソース識別子から前記ネットワークを介してリソースを得られた場合はユーザを認証し、前記暗号化したリソース識別子が得られない場合又は前記暗号化したリソース識別子が正しく復号されない場合又は前記復号したリソース識別子から前記ネットワークを介してリソースを得られない場合はユーザを認証しないため、下記のような効果を奏する。

【0094】上記請求項1及び請求項2の発明と同様に、暗号化及び復号の手続きを節約できる、認証のための公開鍵または秘密鍵を配布する手続きを節約できる、パスワードの盗難といった危険を回避することが可能になる、通信回数が軽減される等の効果がある。

【0095】請求項5の発明によれば、情報処理装置は、パスワードを復号鍵として記憶可能であるため、下記のような効果を奏する。

【0096】上記請求項1乃至請求項4の発明と同様の効果があるばかりでなく、パスワードを用いた認証機構

(11)

特開平11-205307

に対して、パスワードをアクセス毎に入力する手間が軽減されるという効果がある。即ち、上述した従来技術と比較すると、本発明では、クライアントがパスワードを復号鍵として記憶するので、一回だけクライアントにリソース識別子と復号鍵を登録すると、次回からはユーザがパスワードを入力する必要がなくなるという効果がある。

【0097】また、パスワードを用いた認証機構に対して、ユーザがパスワードを記憶する必要がなくなるという効果がある。

【0098】また、パスワードを用いた認証機構に対して、ユーザがパスワードを誤入力する恐れがなくなるという効果がある。

【0099】また、パスワードを用いた認証機構に対して、パスワードをネットワークに流すことがなくなるという効果がある。即ち、上述した従来技術と比較すると、本発明では、パスワードや暗号の暗号化鍵、復号鍵そのものはネットワークに流れないため、従来技術のようなパスワードの盗難といった危険を回避することが可能になるという効果がある。

【0100】請求項6の発明によれば、情報処理装置は、リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読み取り記憶する識別子管理手段を有し、前記リソース識別子は、World Wide Webサーバのアドレスを示すURLであるため、下記のような効果を奏する。

【0101】リソース識別子としてURLを利用した場合においても、リソース識別子(URL)の暗号化及び復号を行うことで、上記請求項1乃至請求項5の発明と同様に、データそのものを暗号化したり復号したりする必要がないため、暗号化及び復号の手続きを節約できる、認証のための公開鍵または秘密鍵を配布する手続きを節約できる、パスワードの盗難といった危険を回避することが可能になる、パスワードを記憶する必要や誤入力する恐れがなくなる、通信回数が軽減される等の効果がある。

【0102】請求項7の発明によれば、ネットワークを介してサーバ及びクライアント間で通信可能なネットワークシステムであって、前記クライアント側は、前記ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化手段と、暗号化したリソース識別子を復号鍵に基づき復号する復号手段とを有するため、下記のような効果を奏する。

【0103】データそのものを暗号化したり復号したりする必要がないため、暗号化及び復号の手続きを節約できると共に、認証のための公開鍵または秘密鍵を配布する手続きを節約できるという効果がある。

【0104】また、パスワードを用いた認証機構に対して、パスワードをネットワークに流すことがなくなるという効果がある。即ち、上述した従来技術と比較する

と、本発明では、パスワードや暗号の暗号化鍵、復号鍵そのものはネットワークに流れないため、従来技術のようなパスワードの盗難といった危険を回避することが可能になるという効果がある。

【0105】請求項8の発明によれば、ネットワークシステムの前記クライアント側は、前記サーバに対しリソース識別子を用いてデータ配達を要求するデータ要求手段と、前記復号したリソース識別子が正しい場合はリソース識別子を前記サーバに送信し、前記復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御手段とを有し、前記サーバ側は、前記ネットワークの上位装置名、アドレス、通信手段を管理するネットワーク管理手段と、該ネットワーク管理手段による通信でデータを配達するデータ配達手段と、サーバ上のデータを管理するデータ管理手段とを有するため、下記のような効果を奏する。

【0106】上記請求項7の発明と同様の効果があるばかりでなく、パスワードを用いた認証機構に対して、ネットワークの通信回数を減らすことにより、ネットワークのトラフィック(通信量)及び通信時間を軽減できるという効果がある。即ち、上述した従来技術と比較すると、本発明では、暗号化されたリソース識別子を使用する場合は、クライアントがリソース識別子を復号し、正しければ復号したリソース識別子をサーバに送信し、正しくなければリソース識別子を送信しないため、通信回数が軽減されるという効果がある。

【0107】請求項9の発明によれば、ネットワークシステムの前記クライアント側は、ユーザの認証を行うユーザ認証手段を有するため、下記のような効果を奏する。

【0108】上記請求項7及び請求項8の発明と同様に、暗号化及び復号の手続きを節約できる、認証のための公開鍵または秘密鍵を配布する手続きを節約できる、パスワードの盗難といった危険を回避することが可能になる、通信回数が軽減される等の効果がある。

【0109】請求項10の発明によれば、ネットワークシステムのクライアント側の前記ユーザ認証手段は、前記暗号化したリソース識別子が正しく復号された場合で且つ前記復号したリソース識別子から前記ネットワークを介してリソースを得られた場合はユーザを認証し、前記暗号化したリソース識別子が得られない場合又は前記暗号化したリソース識別子が正しく復号されない場合又は前記復号したリソース識別子から前記ネットワークを介してリソースを得られない場合はユーザを認証しないため、下記のような効果を奏する。

【0110】上記請求項7及び請求項8の発明と同様に、暗号化及び復号の手続きを節約できる、認証のための公開鍵または秘密鍵を配布する手続きを節約できる、パスワードの盗難といった危険を回避することが可能になる、通信回数が軽減される等の効果がある。

(12)

特開平 11-205307

【0111】請求項11の発明によれば、ネットワークシステムの前記クライアント側は、パスワードを復号鍵として記憶可能であるため、下記のような効果を奏する。

【0112】上記請求項7乃至請求項10の発明と同様の効果があるばかりでなく、パスワードを用いた認証機構に対して、パスワードをアクセス毎に入力する手間が軽減されるという効果がある。即ち、上述した従来技術と比較すると、本発明では、クライアントがパスワードを復号鍵として記憶するので、一回だけクライアントにリソース識別子と復号鍵を登録すると、次回からはユーザがパスワードを入力する必要がなくなるという効果がある。

【0113】また、パスワードを用いた認証機構に対して、ユーザがパスワードを記憶する必要がなくなるという効果がある。

【0114】また、パスワードを用いた認証機構に対して、ユーザがパスワードを誤入力する恐れがなくなるという効果がある。

【0115】また、パスワードを用いた認証機構に対して、パスワードをネットワークに流すことがなくなるという効果がある。即ち、上述した従来技術と比較すると、本発明では、パスワードや暗号の暗号化鍵、復号鍵そのものはネットワークに流れないため、従来技術のようなパスワードの盗難といった危険を回避することが可能になるという効果がある。

【0116】請求項12の発明によれば、ネットワークシステムの前記クライアント側は、リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読み取り記憶する識別子管理手段を有し、前記リソース識別子は、World Wide Webサーバのアドレスを示すURLであるため、下記のような効果を奏する。

【0117】リソース識別子としてURLを利用した場合においても、リソース識別子(URL)の暗号化及び復号を行うことで、上記請求項7乃至請求項11の発明と同様に、データそのものを暗号化したり復号したりする必要がないため、暗号化及び復号の手続きを節約できる、認証のための公開鍵または秘密鍵を配布する手続きを節約できる、パスワードの盗難といった危険を回避することが可能になる、パスワードを記憶する必要や誤入力する恐れがなくなる、通信回数が軽減される等の効果がある。

【0118】請求項13の発明によれば、ネットワークを介してサーバと通信可能な情報処理装置におけるリソース識別子変換方法であって、前記ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化ステップと、暗号化したリソース識別子を復号鍵に基づき復号する復号ステップとを有するため、下記のような効果を奏する。

【0119】データそのものを暗号化したり復号したりする必要がないため、暗号化及び復号の手続きを節約できると共に、認証のための公開鍵または秘密鍵を配布する手続きを節約できるという効果がある。

【0120】また、パスワードを用いた認証機構に対して、パスワードをネットワークに流すことがなくなるという効果がある。即ち、上述した従来技術と比較すると、本発明では、パスワードや暗号の暗号化鍵、復号鍵そのものはネットワークに流れないため、従来技術のようなパスワードの盗難といった危険を回避することが可能になるという効果がある。

【0121】請求項14の発明によれば、リソース識別子変換方法は、前記サーバに対しリソース識別子を用いてデータ配達を要求するデータ読出ステップと、前記復号したリソース識別子が正しい場合はリソース識別子を前記サーバに送信し、前記復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御ステップとを有するため、下記のような効果を奏する。

【0122】上記請求項13の発明と同様の効果があるばかりでなく、パスワードを用いた認証機構に対して、ネットワークの通信回数を減らすことにより、ネットワークのトラフィック(通信量)及び通信時間を軽減できるという効果がある。即ち、上述した従来技術と比較すると、本発明では、暗号化されたリソース識別子を使用する場合は、クライアントがリソース識別子を復号し、正しければ復号したリソース識別子をサーバに送信し、正しくなければリソース識別子を送信しないため、通信回数が軽減されるという効果がある。

【0123】請求項15の発明によれば、リソース識別子変換方法は、ユーザの認証を行うユーザ認証ステップを有するため、下記のような効果を奏する。

【0124】上記請求項13及び請求項14の発明と同様に、暗号化及び復号の手続きを節約できる、認証のための公開鍵または秘密鍵を配布する手続きを節約できる、パスワードの盗難といった危険を回避することが可能になる、通信回数が軽減される等の効果がある。

【0125】請求項16の発明によれば、リソース識別子変換方法の前記ユーザ認証ステップでは、前記暗号化したリソース識別子が正しく復号された場合で且つ前記復号したリソース識別子から前記ネットワークを介してリソースを得られた場合はユーザを認証し、前記暗号化したリソース識別子が得られない場合又は前記暗号化したリソース識別子が正しく復号されない場合又は前記復号したリソース識別子から前記ネットワークを介してリソースを得られない場合はユーザを認証しないため、下記のような効果を奏する。

【0126】上記請求項13及び請求項14の発明と同様に、暗号化及び復号の手続きを節約できる、認証のための公開鍵または秘密鍵を配布する手続きを節約でき

(13)

特開平11-205307

る、パスワードの盗難といった危険を回避することが可能になる、通信回数が軽減される等の効果がある。

【0127】請求項17の発明によれば、リソース識別子変換方法では、パスワードを復号鍵として記憶可能であるため、下記のような効果を奏する。

【0128】上記請求項13乃至請求項16の発明と同様の効果があるばかりでなく、パスワードを用いた認証機構に対して、パスワードをアクセス毎に入力する手間が軽減されるという効果がある。即ち、上述した従来技術と比較すると、本発明では、クライアントがパスワードを復号鍵として記憶するので、一回だけクライアントにリソース識別子と復号鍵を登録すると、次回からはユーザがパスワードを入力する必要がなくなるという効果がある。

【0129】また、パスワードを用いた認証機構に対して、ユーザがパスワードを記憶する必要がなくなるという効果がある。

【0130】また、パスワードを用いた認証機構に対して、ユーザがパスワードを誤入力する恐れがなくなるという効果がある。

【0131】また、パスワードを用いた認証機構に対して、パスワードをネットワークに流すことがなくなるという効果がある。即ち、上述した従来技術と比較すると、本発明では、パスワードや暗号の暗号化鍵、復号鍵そのものはネットワークに流れないため、従来技術のようなパスワードの盗難といった危険を回避することが可能になるという効果がある。

【0132】請求項18の発明によれば、リソース識別子変換方法は、リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読み取り記憶する識別子管理ステップを有し、前記リソース識別子は、World Wide Webサーバのアドレスを示すURLであるため、下記のような効果を奏する。

【0133】リソース識別子としてURLを利用した場合においても、リソース識別子(URL)の暗号化及び復号を行うことで、上記請求項13乃至請求項17の発明と同様に、データそのものを暗号化したり復号したりする必要がないため、暗号化及び復号の手続きを節約できる、認証のための公開鍵または秘密鍵を配布する手続きを節約できる、パスワードの盗難といった危険を回避することが可能になる、パスワードを記憶する必要や誤入力する恐れがなくなる、通信回数が軽減される等の効果がある。

【0134】請求項19の発明によれば、ネットワークを介してサーバと通信可能な情報処理装置に供給可能な記憶媒体であって、前記ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化ステップと、暗号化したリソース識別子を復号鍵に基づき復号する復号ステップとを有するプログラムを記憶しているため、下記のような効果を奏する。

【0135】データそのものを暗号化したり復号したりする必要がないため、暗号化及び復号の手続きを節約できると共に、認証のための公開鍵または秘密鍵を配布する手続きを節約できるという効果がある。

【0136】また、パスワードを用いた認証機構に対して、パスワードをネットワークに流すことになると、いう効果がある。即ち、上述した従来技術と比較すると、本発明では、パスワードや暗号の暗号化鍵、復号鍵そのものはネットワークに流れないため、従来技術のようなパスワードの盗難といった危険を回避することが可能になるという効果がある。

【0137】請求項20の発明によれば、記憶媒体の前記プログラムは、前記サーバに対しリソース識別子を用いてデータ配信を要求するデータ読出ステップと、前記復号したリソース識別子が正しい場合はリソース識別子を前記サーバに送信し、前記復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御ステップとを有するため、下記のような効果を奏する。

【0138】上記請求項19の発明と同様の効果があるばかりでなく、パスワードを用いた認証機構に対して、ネットワークの通信回数を減らすことにより、ネットワークのトラフィック(通信量)及び通信時間を軽減できるという効果がある。即ち、上述した従来技術と比較すると、本発明では、暗号化されたリソース識別子を使用する場合は、クライアントがリソース識別子を復号し、正しければ復号したリソース識別子をサーバに送信し、正しくなければリソース識別子を送信しないため、通信回数が軽減されるという効果がある。

【0139】請求項21の発明によれば、記憶媒体の前記プログラムは、ユーザの認証を行うユーザ認証ステップを有するため、下記のような効果を奏する。

【0140】上記請求項19及び請求項20の発明と同様に、暗号化及び復号の手続きを節約できる、認証のための公開鍵または秘密鍵を配布する手続きを節約できる、パスワードの盗難といった危険を回避することが可能になる、通信回数が軽減される等の効果がある。

【0141】請求項22の発明によれば、記憶媒体の前記ユーザ認証ステップでは、前記暗号化したリソース識別子が正しく復号された場合で且つ前記復号したリソース識別子から前記ネットワークを介してリソースを得られた場合はユーザを認証し、前記暗号化したリソース識別子が得られない場合又は前記暗号化したリソース識別子が正しく復号されない場合又は前記復号したリソース識別子から前記ネットワークを介してリソースを得られない場合はユーザを認証しないため、下記のような効果を奏する。

【0142】上記請求項19及び請求項20の発明と同様に、暗号化及び復号の手続きを節約できる、認証のための公開鍵または秘密鍵を配布する手続きを節約でき

(14)

特開平 11-205307

る、パスワードの盗難といった危険を回避することが可能になる、通信回数が軽減される等の効果がある。

【0143】請求項23の発明によれば、記憶媒体は、パスワードを復号鍵として記憶可能であるため、下記のような効果を奏する。

【0144】上記請求項19乃至請求項22の発明と同様の効果があるばかりでなく、パスワードを用いた認証機構に対して、パスワードをアクセス毎に入力する手間が軽減されるという効果がある。即ち、上述した従来技術と比較すると、本発明では、クライアントがパスワードを復号鍵として記憶するので、一回だけクライアントにリソース識別子と復号鍵を登録すると、次回からはユーザがパスワードを入力する必要がなくなるという効果がある。

【0145】また、パスワードを用いた認証機構に対して、ユーザがパスワードを記憶する必要がなくなるという効果がある。

【0146】また、パスワードを用いた認証機構に対して、ユーザがパスワードを誤入力する恐れがなくなるという効果がある。

【0147】また、パスワードを用いた認証機構に対して、パスワードをネットワークに流すことがなくなるという効果がある。即ち、上述した従来技術と比較すると、本発明では、パスワードや暗号の暗号化鍵、復号鍵そのものはネットワークに流れないので、従来技術のようなパスワードの盗難といった危険を回避することが可能になるという効果がある。

【0148】請求項24の発明によれば、記憶媒体の前記プログラムは、リソース識別子の入力を促す旨を表示すると共に入力されたりソース識別子を読み取り記憶する識別子管理ステップを有し、前記リソース識別子は、World Wide Webサーバのアドレスを示すURLであるため、下記のような効果を奏する。

【0149】リソース識別子としてURLを利用した場合においても、リソース識別子(URL)の暗号化及び復号を行うことで、上記請求項19乃至請求項23の発明と同様に、データそのものを暗号化したり復号したりする必要がないため、暗号化及び復号の手続きを節約できる、認証のための公開鍵または秘密鍵を配布する手続きを節約できる、パスワードの盗難といった危険を回避することが可能になる、パスワードを記憶する必要や誤入力する恐れがなくなる、通信回数が軽減される等の効果がある。

【図面の簡単な説明】

【図1】本発明の第1及び第2の実施の形態に係る情報処理装置(クライアント)及び外部装置(サーバ)からなるネットワークシステムの要部の構成を示すと共に特許請求の範囲に対応させた機能ブロック図である。

【図2】本発明の第1及び第2の実施の形態に係る情報処理装置の構成を示すブロック図である。

【図3】本発明の第1及び第2の実施の形態に係る情報処理装置(クライアント)及び外部装置(サーバ)からなるネットワークシステムの構成を示すブロック図である。

【図4】本発明の第1の実施の形態に係る情報処理装置における処理を示すフローチャートである。

【図5】本発明の第2の実施の形態に係る情報処理装置における処理を示すフローチャートである。

【図6】本発明の第1及び第2の実施の形態に係るプログラム及び関連データを記憶した記憶媒体の記憶内容の構成例を示す説明図である。

【図7】本発明の第1及び第2の実施の形態に係るプログラム及び関連データが記憶媒体から情報処理装置に供給される概念例を示す説明図である。

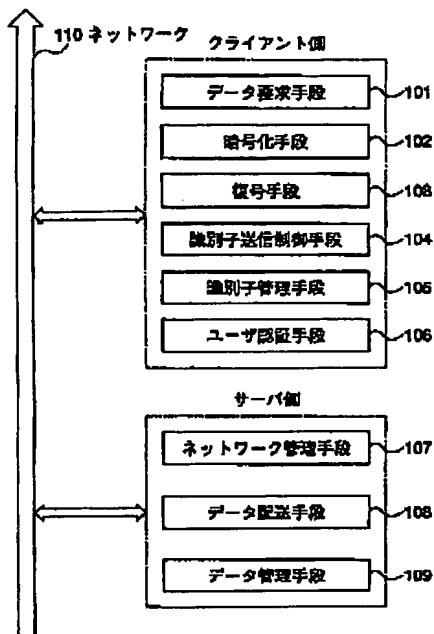
【符号の説明】

- 101 データ要求手段
- 102 暗号化手段
- 103 復号手段
- 104 識別子送信制御手段
- 105 識別子管理手段
- 106 ユーザ認証手段
- 107 ネットワーク管理手段
- 108 データ配達手段
- 109 データ管理手段
- 110, 307 ネットワーク
- 201 入力部
- 202 中央演算処理部
- 206 出力部
- 301 クライアントプログラム
- 302 暗号化プログラム
- 303 暗号化鍵
- 304 復号プログラム
- 305 復号鍵
- 306, 308 ネットワークインターフェース
- 309 サーバプログラム
- 310 送信データ

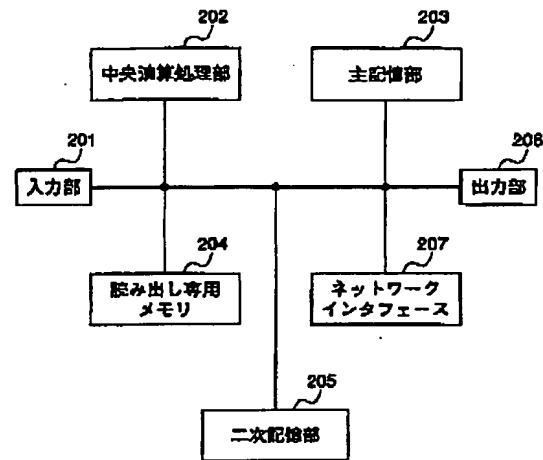
(15)

特開平11-205307

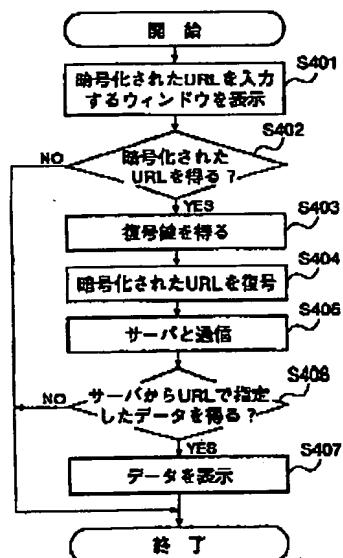
【図1】



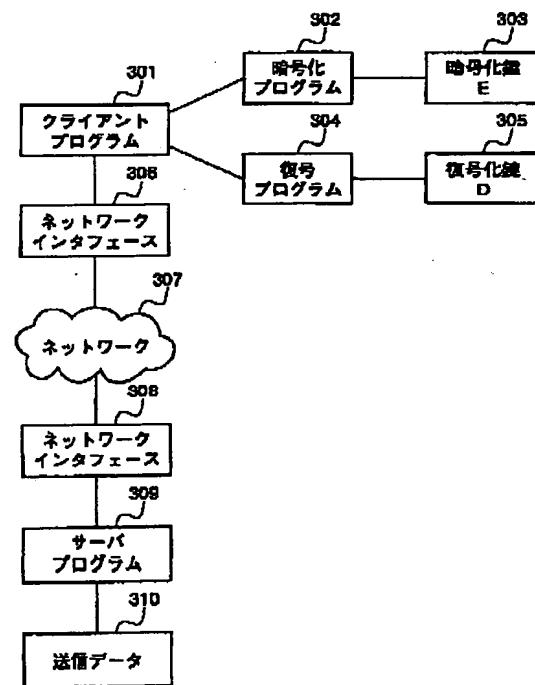
【図2】



【図4】



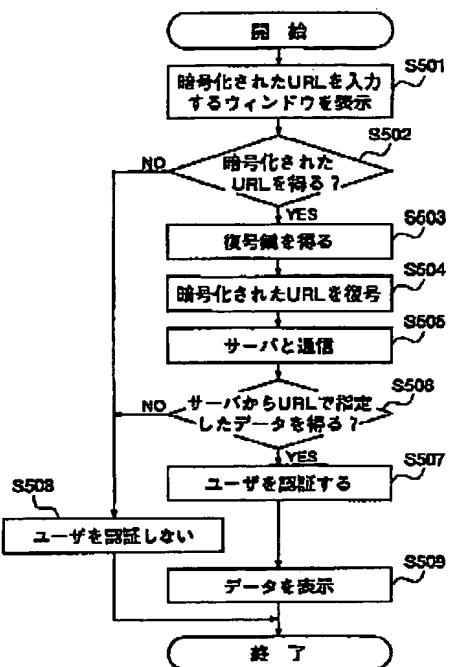
【図3】



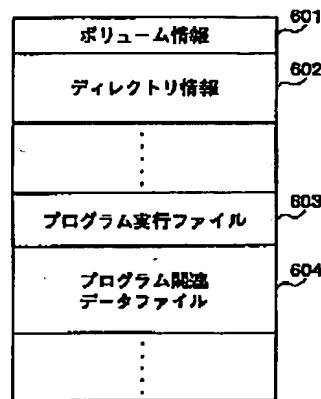
(16)

特開平 11-205307

【図5】



【図6】



【図7】

